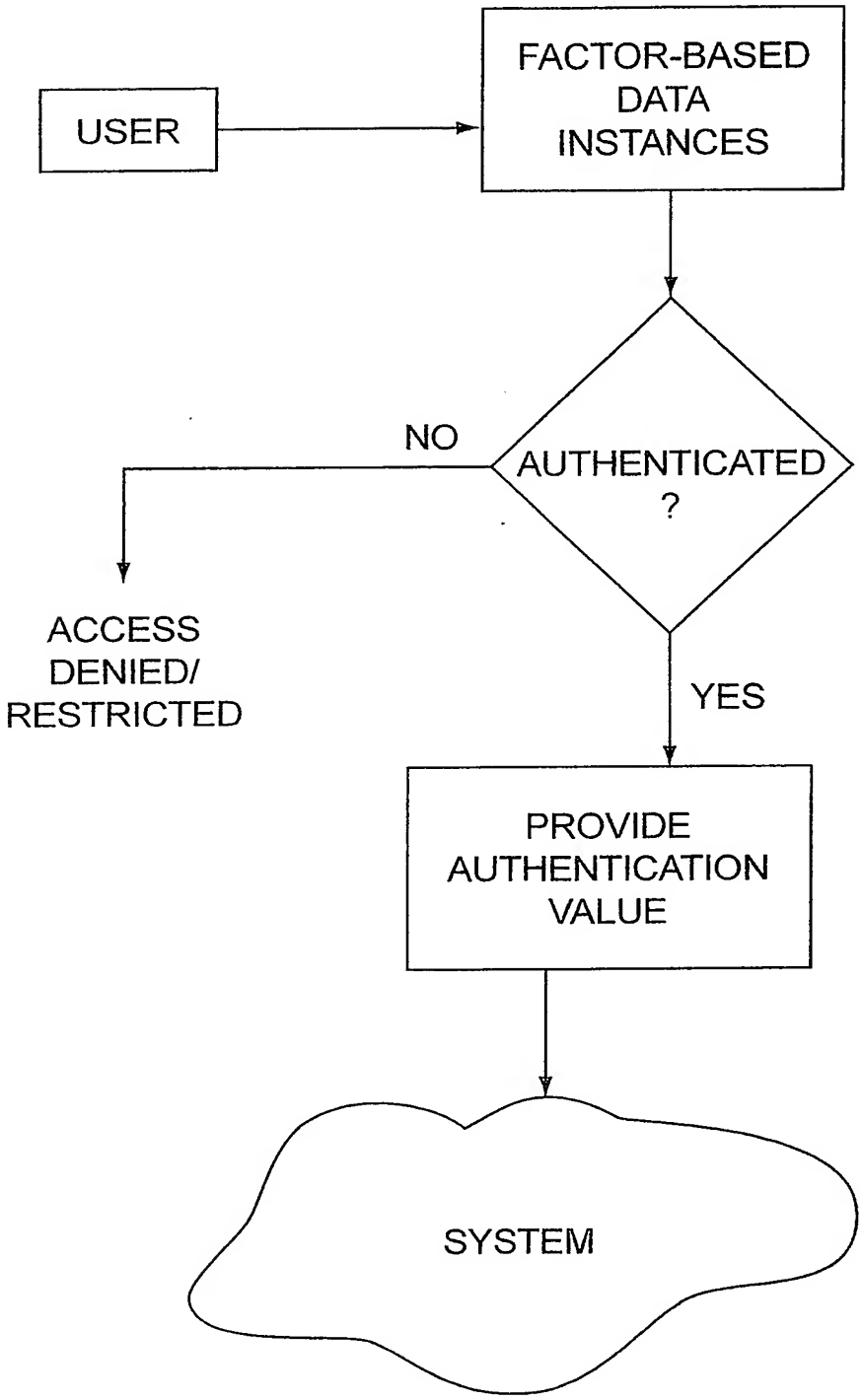


FIG. 1

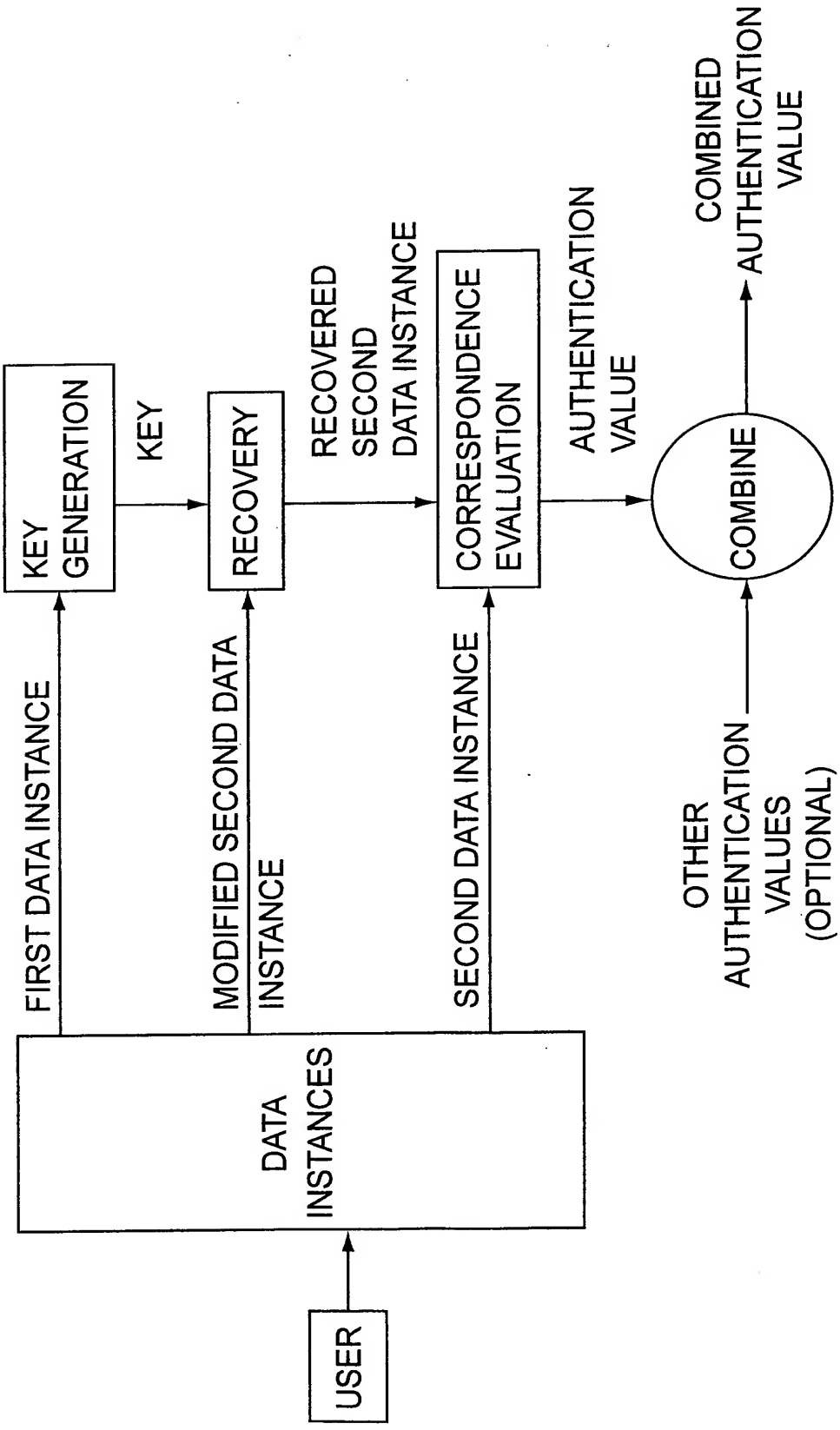

USER
DATA INSTANCES
FIRST DATA INSTANCE
KEY GENERATION
KEY
MODIFIED SECOND DATA INSTANCE
RECOVERY
RECOVERED SECOND DATA INSTANCE
SECOND DATA INSTANCE
CORRESPONDENCE EVALUATION
AUTHENTICATION VALUE
OTHER AUTHENTICATION VALUES (OPTIONAL)
COMBINE
COMBINED AUTHENTICATION VALUE

FIG. 2

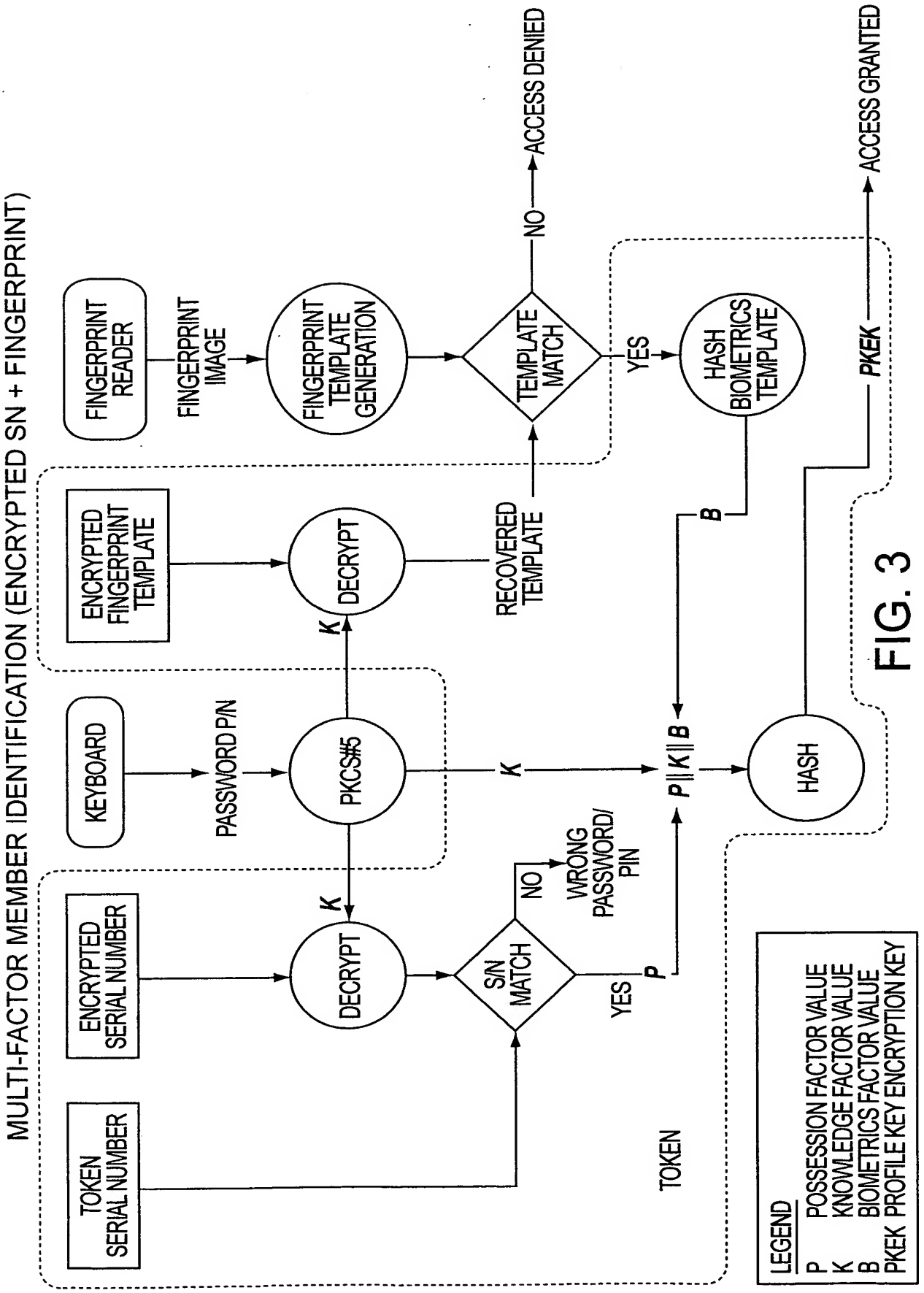

MULTI-FACTOR MEMBER IDENTIFICATION (ENCRYPTED SN + FINGERPRINT)
TOKEN SERIAL NUMBER
ENCRYPTED SERIAL NUMBER
KEYBOARD
PASSWORD P/N
PKCS#5
K
DECRYPT
S/N MATCH
NO
WRONG PASSWORD/ PIN
YES
P
K
P||K||B
HASH
PKEK
ACCESS GRANTED
ENCRYPTED FINGERPRINT TEMPLATE
DECRYPT
RECOVERED TEMPLATE
TEMPLATE MATCH
NO
ACCESS DENIED
YES
B
HASH BIOMETRICS TEMPLATE
FINGERPRINT READER
FINGERPRINT IMAGE
FINGERPRINT TEMPLATE GENERATION
TOKEN
LEGEND
P POSSESSION FACTOR VALUE
K KNOWLEDGE FACTOR VALUE
B BIOMETRICS FACTOR VALUE
PKEK PROFILE KEY ENCRYPTION KEY

FIG. 3

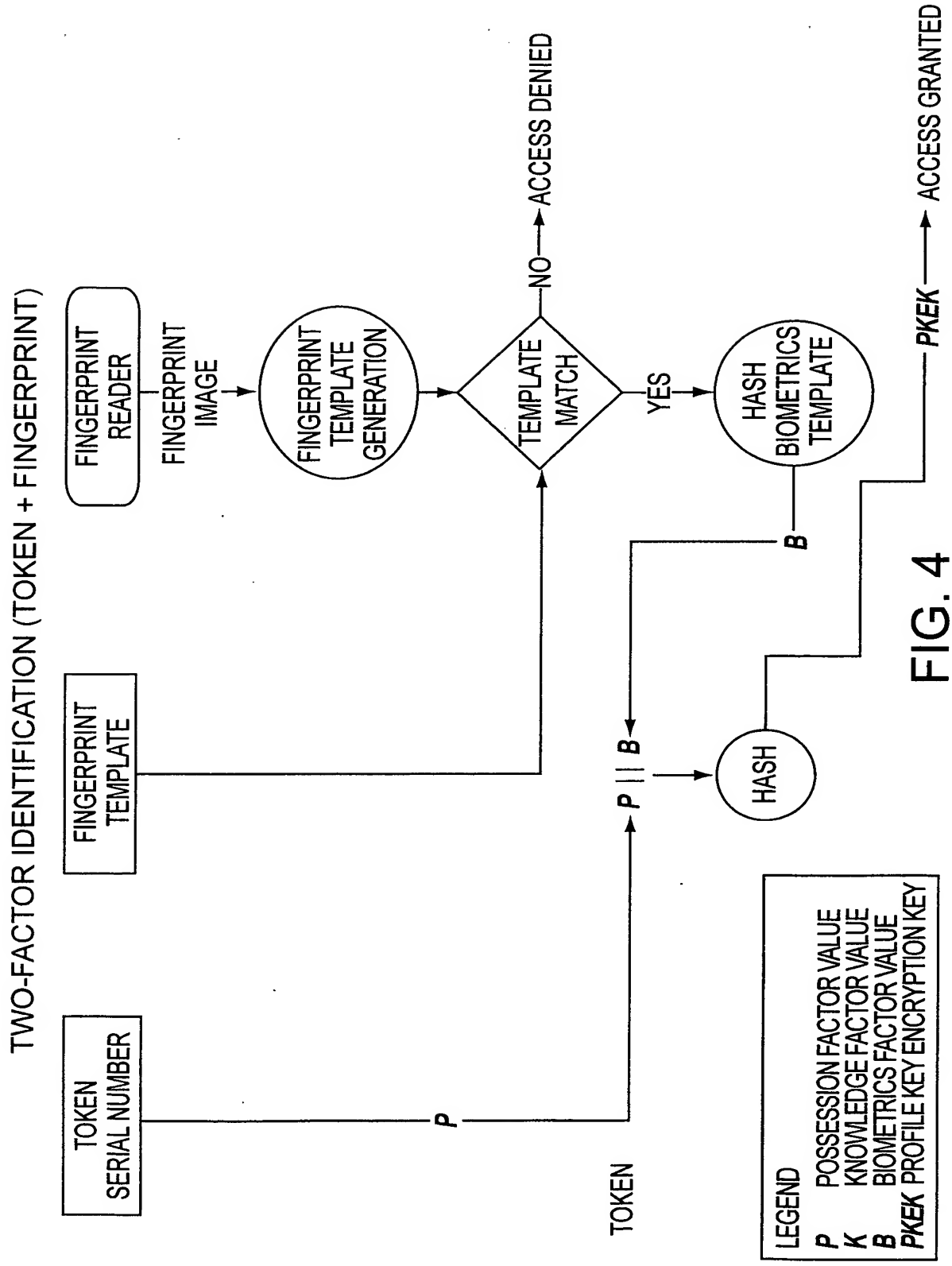

TWO-FACTOR IDENTIFICATION (TOKEN + FINGERPRINT)
FINGERPRINT READER
FINGERPRINT IMAGE
FINGERPRINT TEMPLATE GENERATION
TEMPLATE MATCH
NO
ACCESS DENIED
YES
HASH BIOMETRICS TEMPLATE
PKEK
ACCESS GRANTED
FINGERPRINT TEMPLATE
TOKEN SERIAL NUMBER
P
TOKEN
P || B
HASH
B
LEGEND
P POSSESSION FACTOR VALUE
K KNOWLEDGE FACTOR VALUE
B BIOMETRICS FACTOR VALUE
PKEK PROFILE KEY ENCRYPTION KEY

FIG. 4

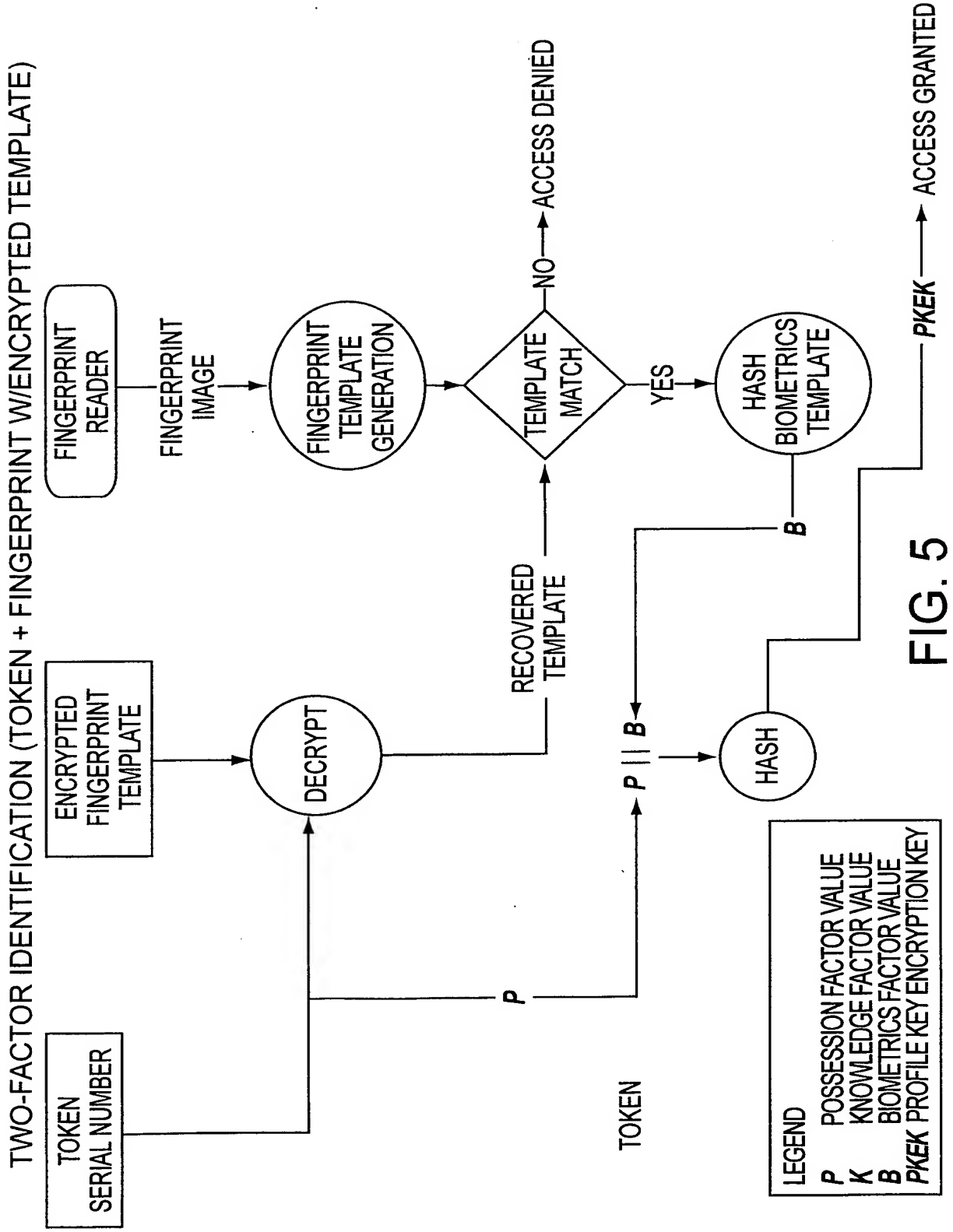

TWO-FACTOR IDENTIFICATION (TOKEN + FINGERPRINT W/ENCRYPTED TEMPLATE)
TOKEN SERIAL NUMBER
ENCRYPTED FINGERPRINT TEMPLATE
FINGERPRINT READER
FINGERPRINT IMAGE
FINGERPRINT TEMPLATE GENERATION
DECRYPT
TEMPLATE MATCH
NO
ACCESS DENIED
YES
HASH BIOMETRICS TEMPLATE
RECOVERED TEMPLATE
P
P || B
B
HASH
PKEK
ACCESS GRANTED
TOKEN
LEGEND
P POSSESSION FACTOR VALUE
K KNOWLEDGE FACTOR VALUE
B BIOMETRICS FACTOR VALUE
PKEK PROFILE KEY ENCRYPTION KEY

FIG. 5

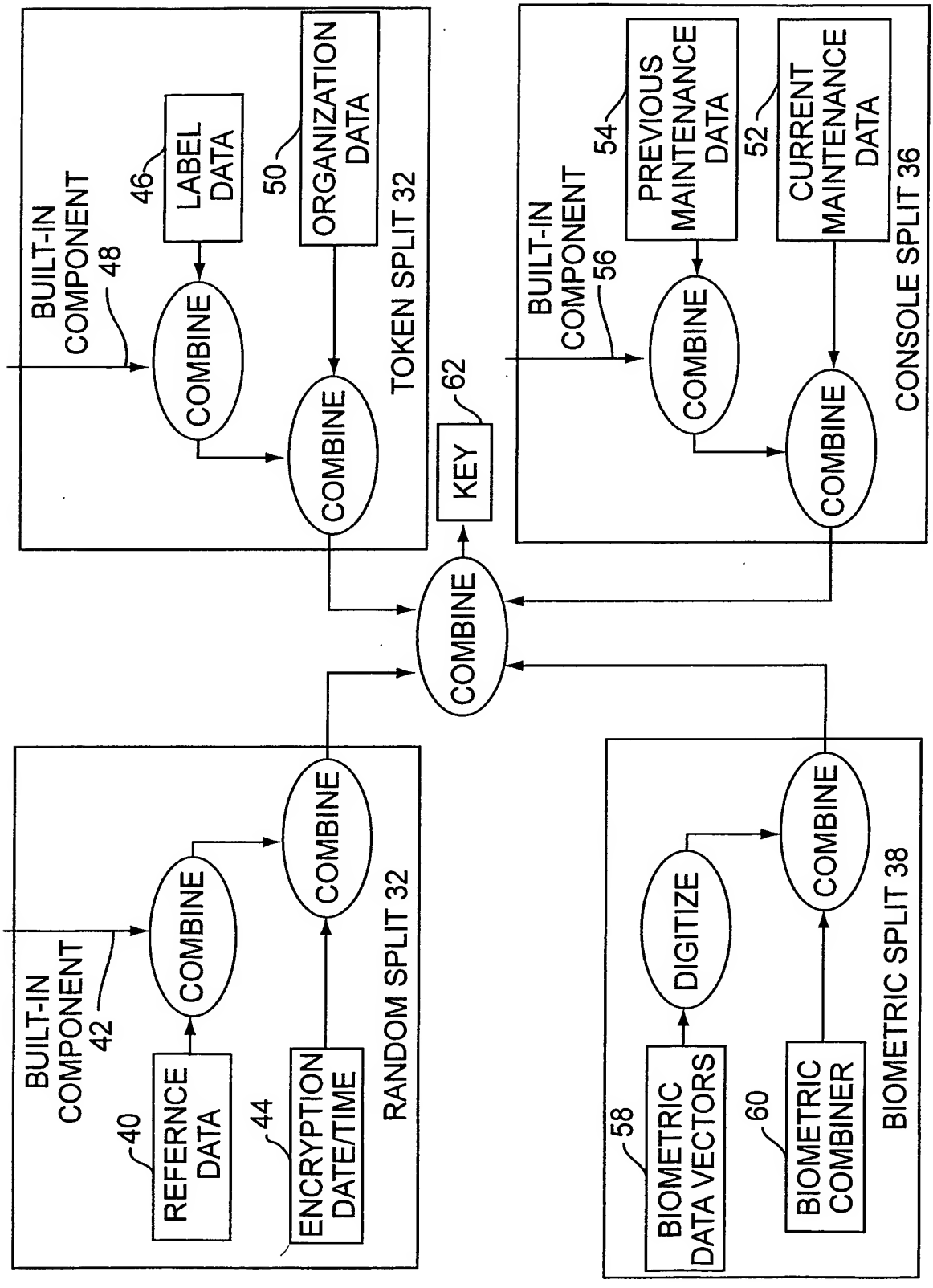

BUILT-IN COMPONENT
48
46
LABEL DATA
50
ORGANIZATION DATA
COMBINE
COMBINE
TOKEN SPLIT 32
KEY
62
BUILT-IN COMPONENT
56
54
PREVIOUS MAINTENANCE DATA
52
CURRENT MAINTENANCE DATA
COMBINE
COMBINE
CONSOLE SPLIT 36
COMBINE
BUILT-IN COMPONENT
42
COMBINE
COMBINE
40
REFERNCE DATA
44
ENCRYPTION DATE/TIME
RANDOM SPLIT 32
DIGITIZE
COMBINE
58
BIOMETRIC DATA VECTORS
60
BIOMETRIC COMBINER
BIOMETRIC SPLIT 38

FIG. 6

NUMBER	DECRYPT	ENCRYPT	NUMBER	DECRYPT	ENCRYPT	NUMBER	DECRYPT	ENCRYPT
1	-	-	4	←	-	7	→	-
2	-	←	5	←	←	8	→	←
3	-	→	6	←	→	9	→	→

FIG. 7

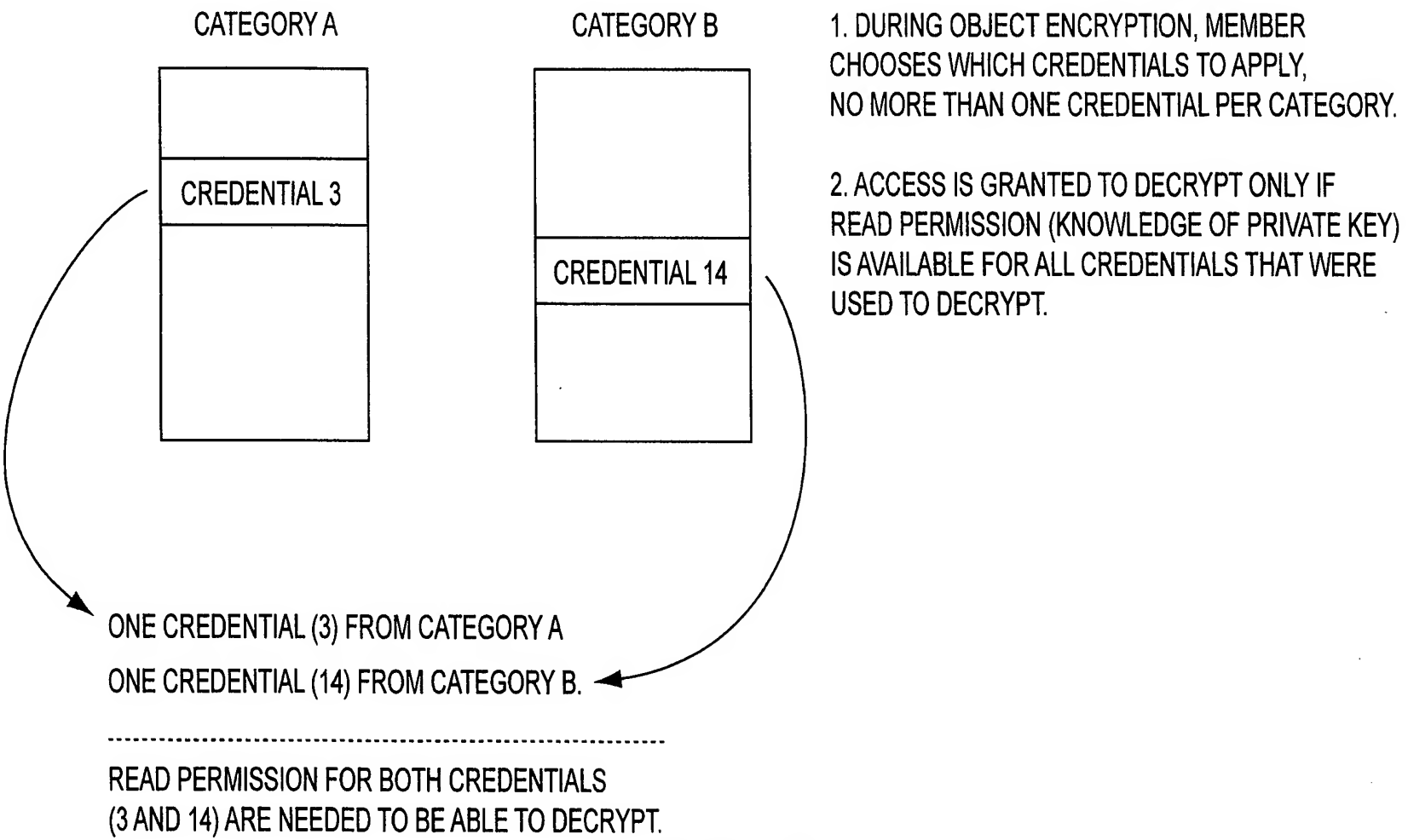
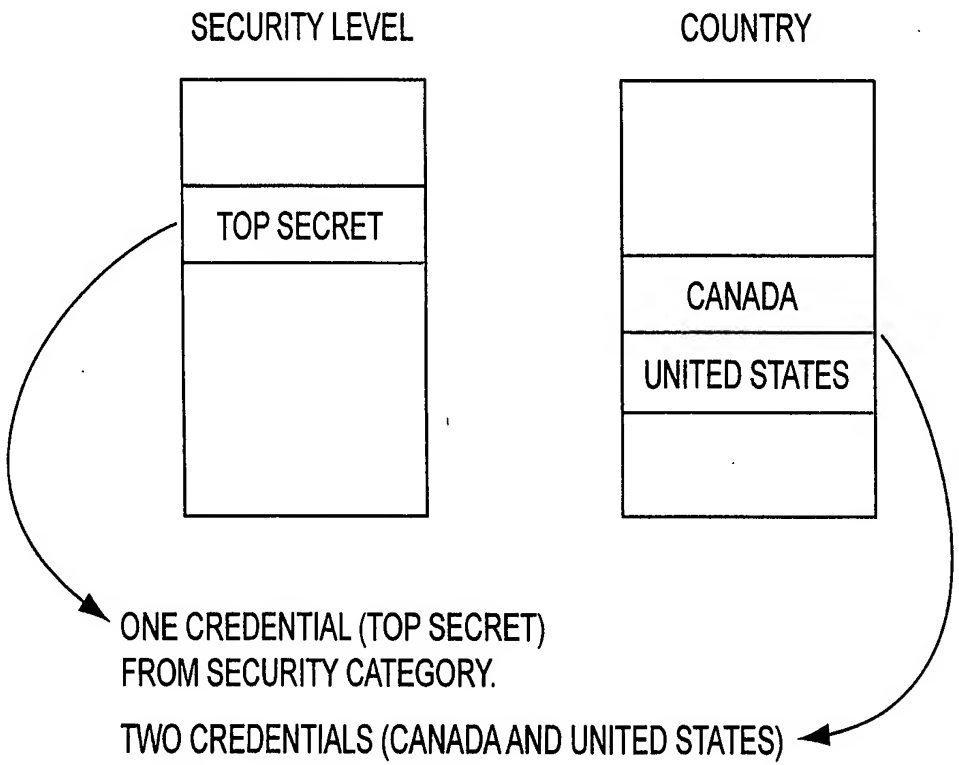

ACCESS RESTRICTED CREDENTIALS
CATEGORY A
CATEGORY B
CREDENTIAL 3
CREDENTIAL 14
1. DURING OBJECT ENCRYPTION, MEMBER CHOOSES WHICH CREDENTIALS TO APPLY, NO MORE THAN ONE CREDENTIAL PER CATEGORY.
2. ACCESS IS GRANTED TO DECRYPT ONLY IF READ PERMISSION (KNOWLEDGE OF PRIVATE KEY) IS AVAILABLE FOR ALL CREDENTIALS THAT WERE USED TO DECRYPT.
ONE CREDENTIAL (3) FROM CATEGORY A
ONE CREDENTIAL (14) FROM CATEGORY B.
READ PERMISSION FOR BOTH CREDENTIALS (3 AND 14) ARE NEEDED TO BE ABLE TO DECRYPT.

FIG. 8

ACCESS BROADENING CREDENTIALS



1. DURING OBJECT ENCRYPTION, MEMBER CHOOSES WHICH CREDENTIALS TO APPLY. MORE THAN ONE CREDENTIAL CAN BE SELECETED WITHIN A CATEGORY IF THAT CATEGORY IS A MULTIPLE CREDENTIAL SELECTION CATEGORY.

2. ACCESS IS GRANTED TO DECRYPT IF READ PERMISSION (KNOWLEDGE OF PRIVATE KEY) IS AVAILABLE FOR ANY ONE CREDENTIAL THAT WAS USED TO ENCRYPT IN A MULTIPLE CREDENTIAL SELECTION CATAGORY.

FIG. 9

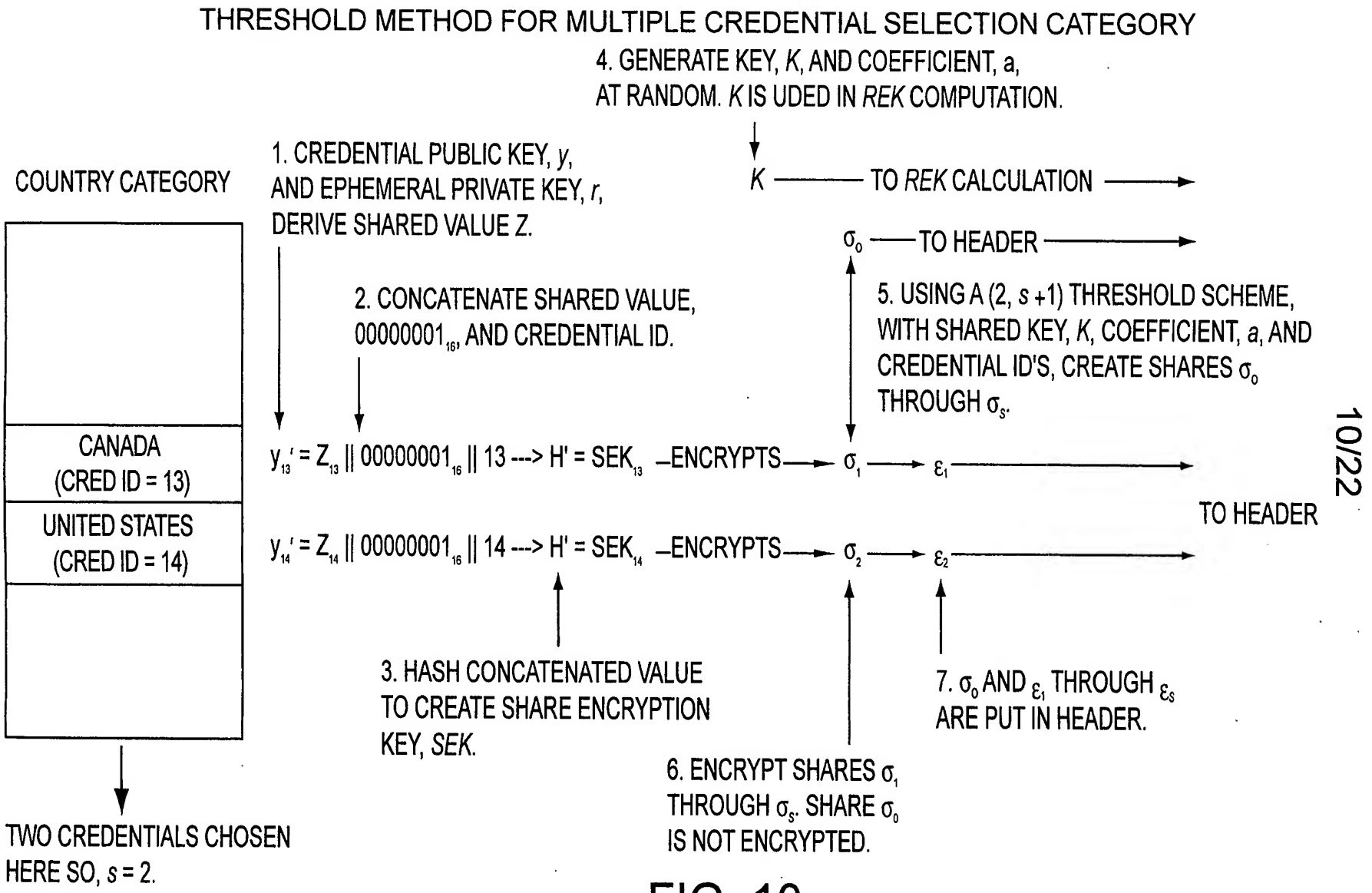

THRESHOLD METHOD FOR MULTIPLE CREDENTIAL SELECTION CATEGORY
4. GENERATE KEY, K, AND COEFFICIENT, a, AT RANDOM. K IS UDED IN REK COMPUTATION.
COUNTRY CATEGORY
1. CREDENTIAL PUBLIC KEY, y, AND EPHEMERAL PRIVATE KEY, r, DERIVE SHARED VALUE Z.
K — TO REK CALCULATION
σ0 — TO HEADER
2. CONCATENATE SHARED VALUE, 00000001 16, AND CREDENTIAL ID.
5. USING A (2, s +1) THRESHOLD SCHEME, WITH SHARED KEY, K, COEFFICIENT, a, AND CREDENTIAL ID'S, CREATE SHARES σ0 THROUGH σs.
CANADA (CRED ID = 13)
UNITED STATES (CRED ID = 14)
y13' = Z13 || 00000001 16 || 13 ---> H' = SEK13 –ENCRYPTS→ σ1 → ε1
TO HEADER
y14' = Z14 || 00000001 16 || 14 ---> H' = SEK14 –ENCRYPTS→ σ2 → ε2
3. HASH CONCATENATED VALUE TO CREATE SHARE ENCRYPTION KEY, SEK.
7. σ0 AND ε1 THROUGH εs ARE PUT IN HEADER.
6. ENCRYPT SHARES σ1 THROUGH σs. SHARE σ0 IS NOT ENCRYPTED.
TWO CREDENTIALS CHOSEN HERE SO, s = 2.

FIG. 10

ACCESS TYPE	SET OF AVAILABLE CREDENTIALS
1	$\{(\forall c \in P \ni. \exists x_c \in c \wedge \lambda_c = \lambda_{IA}) \cup (\forall c \in P \ni. \exists y_c \in c \wedge \lambda_c = \lambda_{IA})\}$
2	$\{(\forall c \in P \ni. \exists x_c \in c \wedge \lambda_c = \lambda_{IA}) \cup (\forall c \in P \ni. \exists y_c \in c \wedge \lambda_c \geq \lambda_{IA})\}$
3	$\{(\forall c \in P \ni. \exists x_c \in c \wedge \lambda_c = \lambda_{IA}) \cup (\forall c \in P \ni. \exists y_c \in c \wedge \lambda_c \leq \lambda_{IA})\}$
4	$\{(\forall c \in P \ni. \exists x_c \in c \wedge \lambda_c \geq \lambda_{IA}) \cup (\forall c \in P \ni. \exists y_c \in c \wedge \lambda_c = \lambda_{IA})\}$
5	$\{(\forall c \in P \ni. \exists x_c \in c \wedge \lambda_c \geq \lambda_{IA}) \cup (\forall c \in P \ni. \exists y_c \in c \wedge \lambda_c \geq \lambda_{IA})\}$
6	$\{(\forall c \in P \ni. \exists x_c \in c \wedge \lambda_c \geq \lambda_{IA}) \cup (\forall c \in P \ni. \exists y_c \in c \wedge \lambda_c \leq \lambda_{IA})\}$
7	$\{(\forall c \in P \ni. \exists x_c \in c \wedge \lambda_c \leq \lambda_{IA}) \cup (\forall c \in P \ni. \exists y_c \in c \wedge \lambda_c = \lambda_{IA})\}$
8	$\{(\forall c \in P \ni. \exists x_c \in c \wedge \lambda_c \leq \lambda_{IA}) \cup (\forall c \in P \ni. \exists y_c \in c \wedge \lambda_c \geq \lambda_{IA})\}$
9	$\{(\forall c \in P \ni. \exists x_c \in c \wedge \lambda_c \leq \lambda_{IA}) \cup (\forall c \in P \ni. \exists y_c \in c \wedge \lambda_c \leq \lambda_{IA})\}$

FIG. 11

ACCESS TYPE	Xek_c	yek_c	INDEPENDENT READ VALUE	INDEPENDENT WRITE VALUE
1	$xek_c = \kappa_\lambda$	$yek_c = \kappa_\lambda$	N/A	N/A
2	$xek_c = \kappa_\lambda$	$yek_c = (H^{(\lambda c - 1)}(yek_1)) / 2^{(h-k)}$	N/A	yek_1
3	$xek_c = \kappa_\lambda$	$yek_c = (H^{(s - \lambda c)}(xek_s)) / 2^{(h-k)}$	N/A	yek_s
4	$xek_c = (H^{(\lambda c - 1)}(xek_1)) / 2^{(h-k)}$	$yek_c = \kappa_\lambda$	xek_1	N/A
5	$xek_c = (H^{(\lambda c - 1)}(xek_1)) / 2^{(h-k)}$	$yek_c = (H^{(\lambda c - 1)}(yek_1)) / 2^{(h-k)}$	xek_1	yek_1
6	$xek_c = (H^{(\lambda c - 1)}(xek_1)) / 2^{(h-k)}$	$yek_c = (H^{(s - \lambda c)}(xek_s)) / 2^{(h-k)}$	xek_1	yek_s
7	$xek_c = (H^{(s - \lambda c)}(xek_s)) / 2^{(h-k)}$	$yek_c = \kappa_\lambda$	xek_s	N/A
8	$xek_c = (H^{(s - \lambda c)}(xek_s)) / 2^{(h-k)}$	$Yek_c = (H^{(\lambda c - 1)}(yek_1)) / 2^{(h-k)}$	xek_s	yek_1
9	$xek_c = (H^{(s - \lambda c)}(xek_s)) / 2^{(h-k)}$	$xek_c = (H^{(s - \lambda c)}(xek_s)) / 2^{(h-k)}$	xek_s	yek_s

FIG. 12

PROFILE ENCRYPTION

ENCRYPTED PROFILE ENCRYPTION KEYS	ENCRYPTED CREDENTIAL PRIVATE AND PUBLIC KEY ENCRYPTION KEYS
$ePEK_1 = e(PEK, \kappa_1)$ $ePEK_2 = e(PEK, \kappa_1)$ • • • $ePEK_{\lambda max} = e(PEK, \kappa_{\lambda max})$	$exek_1 = e(xek_1, \kappa_1)$ $eyek_1 = e(yek_1, \kappa_1)$ $exek_2 = e(xek_2, \kappa_2)$ $eyek_2 = e(yek_2, \kappa_2)$ • • • $exek_{\lambda max} = e(xek_{\lambda max}, \kappa_{\lambda max})$ $eyek_{\lambda max} = e(yek_{\lambda max}, \kappa_{\lambda max})$
ENCRYPTED PROFILE	**ENCRYPTED CREDENTIAL PRIVATE AND PUBLIC KEYS**
$eProfile = e(Profile, PEK)$	$ex_1 = e(x_1, xek_{\lambda(1)})$ $ey_1 = e(y_1, yek_{\lambda(1)})$ $ex_2 = e(x_2, xek_{\lambda(2)})$ $ey_2 = e(y_2, yek_{\lambda(2)})$ • • • $ex_n = e(x_n, xek_{\lambda(n)})$ $ey_n = e(y_n, yek_{\lambda(n)})$

FIG. 13

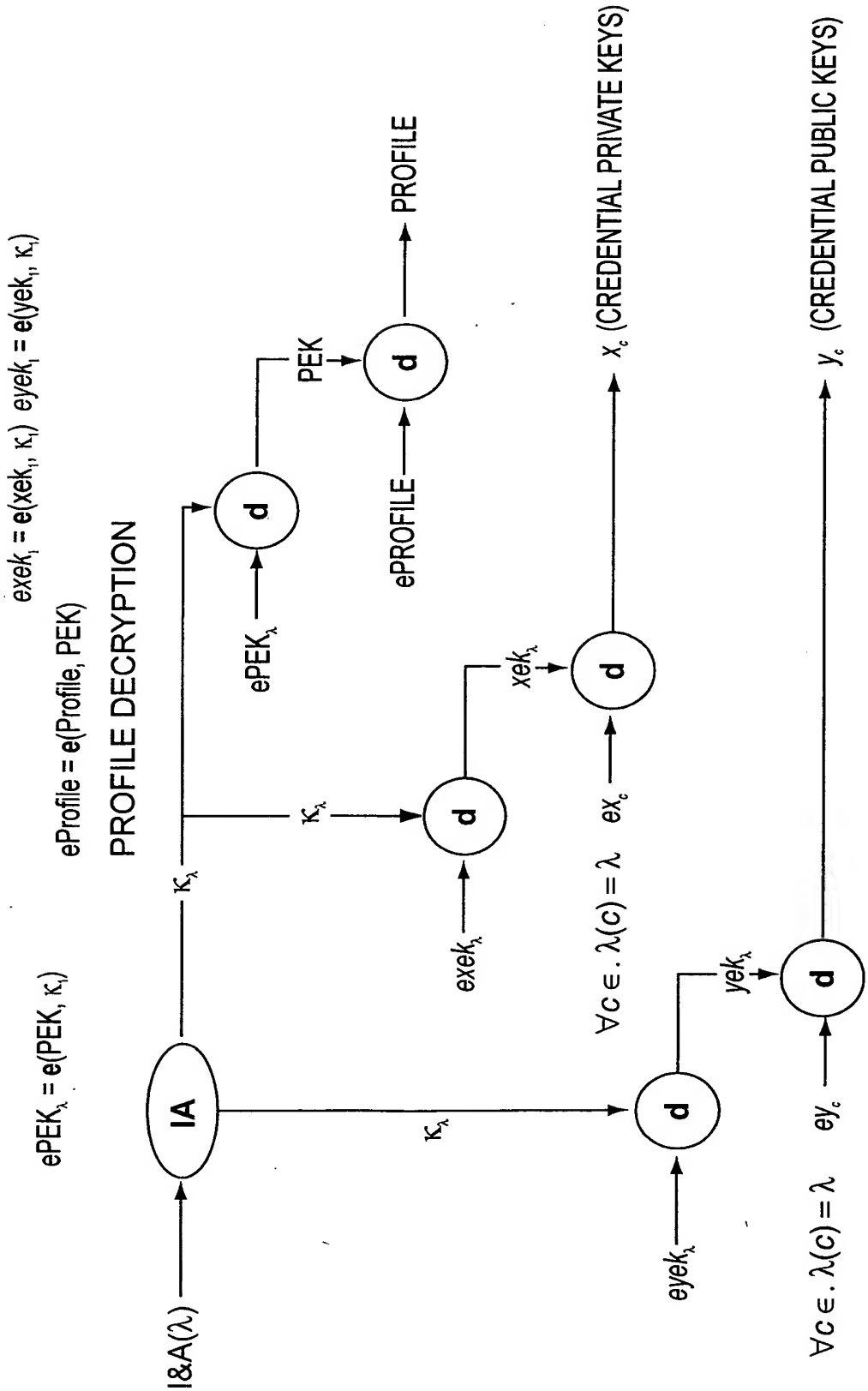

PROFILE DECRYPTION
ePEK$_\lambda$ = e(PEK, κ_ι)
eProfile = e(Profile, PEK)
exek$_\iota$ = e(xek$_\iota$, κ_ι) eyek$_\iota$ = e(yek$_\iota$, κ_ι)
I&A(λ)
IA
κ_λ
ePEK$_\lambda$
d
PEK
ePROFILE
PROFILE
exek$_\lambda$
xek$_\lambda$
∀c ∈ . λ(c) = λ ex$_c$
x$_c$ (CREDENTIAL PRIVATE KEYS)
eyek$_\lambda$
yek$_\lambda$
∀c ∈ . λ(c) = λ ey$_c$
y$_c$ (CREDENTIAL PUBLIC KEYS)

FIG. 14

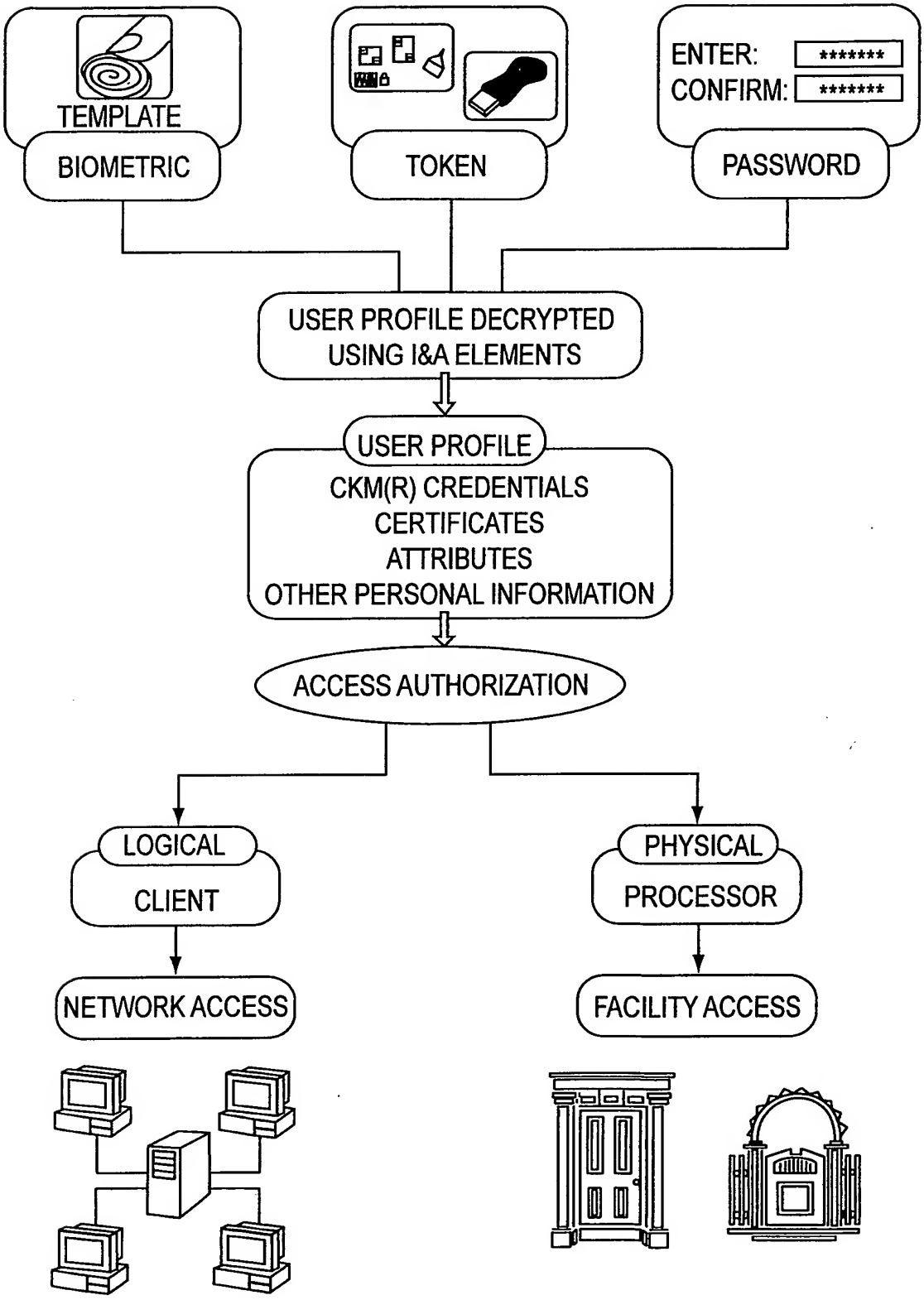

TEMPLATE
BIOMETRIC
TOKEN
ENTER: *******
CONFIRM: *******
PASSWORD
USER PROFILE DECRYPTED USING I&A ELEMENTS
USER PROFILE
CKM(R) CREDENTIALS
CERTIFICATES
ATTRIBUTES
OTHER PERSONAL INFORMATION
ACCESS AUTHORIZATION
LOGICAL
CLIENT
NETWORK ACCESS
PHYSICAL
PROCESSOR
FACILITY ACCESS

FIG. 15

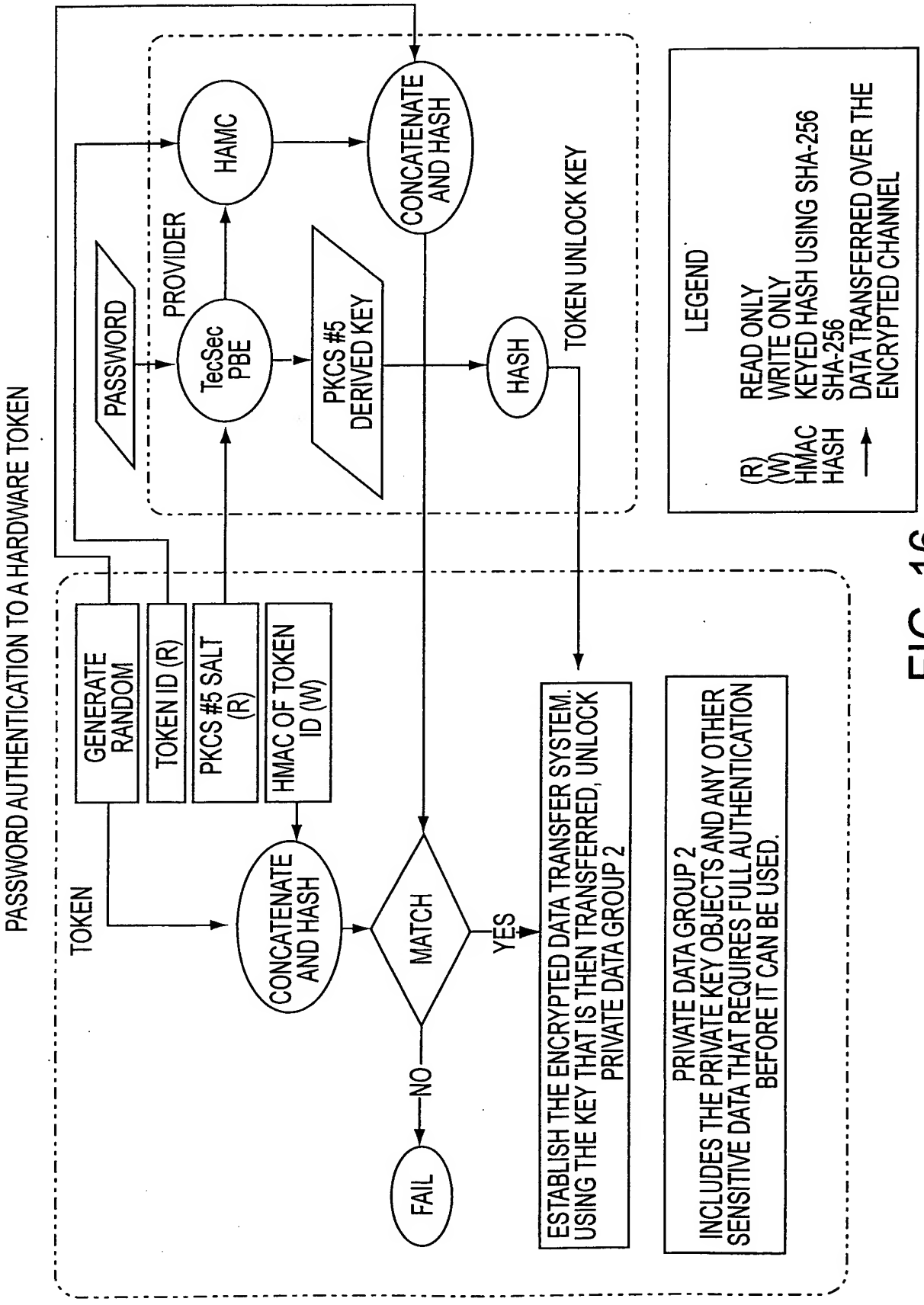

PASSWORD AUTHENTICATION TO A HARDWARE TOKEN
PROVIDER
PASSWORD
TecSec PBE
HAMC
PKCS #5 DERIVED KEY
CONCATENATE AND HASH
HASH
TOKEN UNLOCK KEY
LEGEND
(R) READ ONLY
(W) WRITE ONLY
HMAC KEYED HASH USING SHA-256
HASH SHA-256
DATA TRANSFERRED OVER THE ENCRYPTED CHANNEL
TOKEN
GENERATE RANDOM
TOKEN ID (R)
PKCS #5 SALT (R)
HMAC OF TOKEN ID (W)
CONCATENATE AND HASH
MATCH
YES
NO
FAIL
ESTABLISH THE ENCRYPTED DATA TRANSFER SYSTEM. USING THE KEY THAT IS THEN TRANSFERRED, UNLOCK PRIVATE DATA GROUP 2
PRIVATE DATA GROUP 2
INCLUDES THE PRIVATE KEY OBJECTS AND ANY OTHER SENSITIVE DATA THAT REQUIRES FULL AUTHENTICATION BEFORE IT CAN BE USED.

FIG. 16

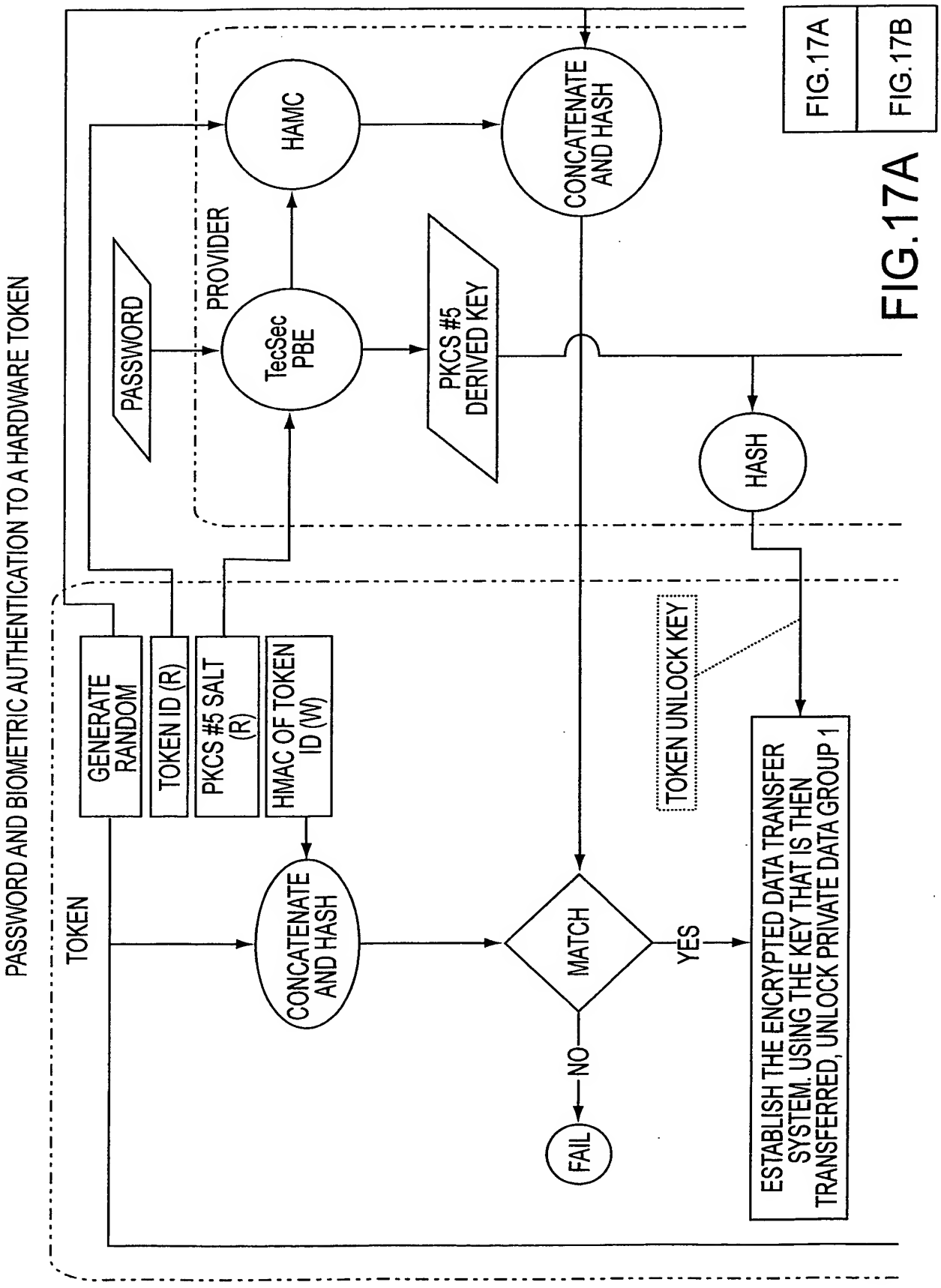

PASSWORD AND BIOMETRIC AUTHENTICATION TO A HARDWARE TOKEN
TOKEN
PROVIDER
PASSWORD
TecSec PBE
HAMC
CONCATENATE AND HASH
PKCS #5 DERIVED KEY
HASH
GENERATE RANDOM
TOKEN ID (R)
PKCS #5 SALT (R)
HMAC OF TOKEN ID (W)
TOKEN UNLOCK KEY
CONCATENATE AND HASH
MATCH
YES
NO
FAIL
ESTABLISH THE ENCRYPTED DATA TRANSFER SYSTEM. USING THE KEY THAT IS THEN TRANSFERRED, UNLOCK PRIVATE DATA GROUP 1
FIG.17A
FIG.17B

FIG.17A

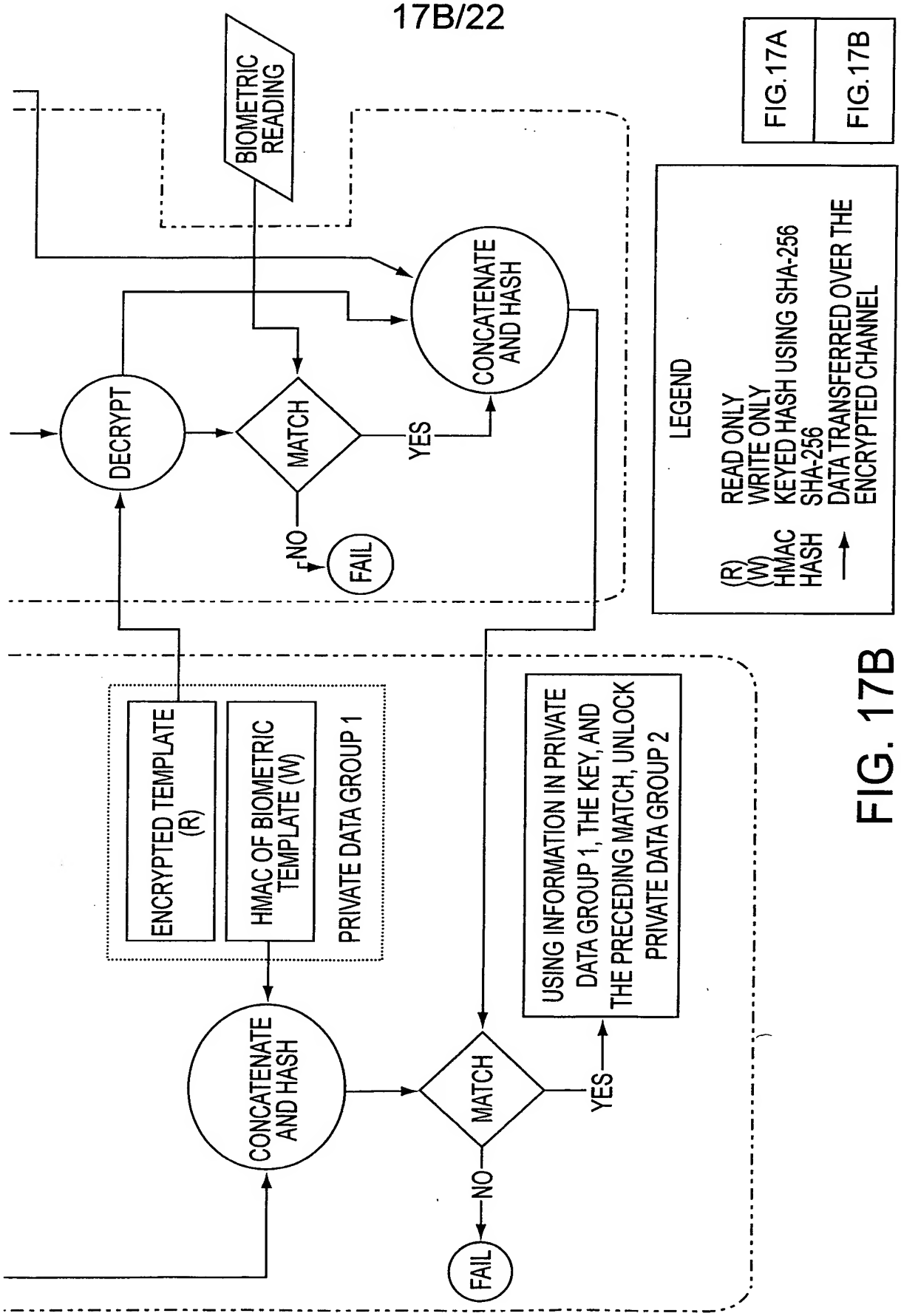

BIOMETRIC READING
DECRYPT
MATCH
YES
NO
FAIL
CONCATENATE AND HASH
ENCRYPTED TEMPLATE (R)
HMAC OF BIOMETRIC TEMPLATE (W)
PRIVATE DATA GROUP 1
CONCATENATE AND HASH
MATCH
YES
NO
FAIL
USING INFORMATION IN PRIVATE DATA GROUP 1, THE KEY, AND THE PRECEDING MATCH, UNLOCK PRIVATE DATA GROUP 2
LEGEND
(R) READ ONLY
(W) WRITE ONLY
HMAC KEYED HASH USING SHA-256
HASH SHA-256
DATA TRANSFERRED OVER THE ENCRYPTED CHANNEL
FIG.17A
FIG.17B

FIG. 17B

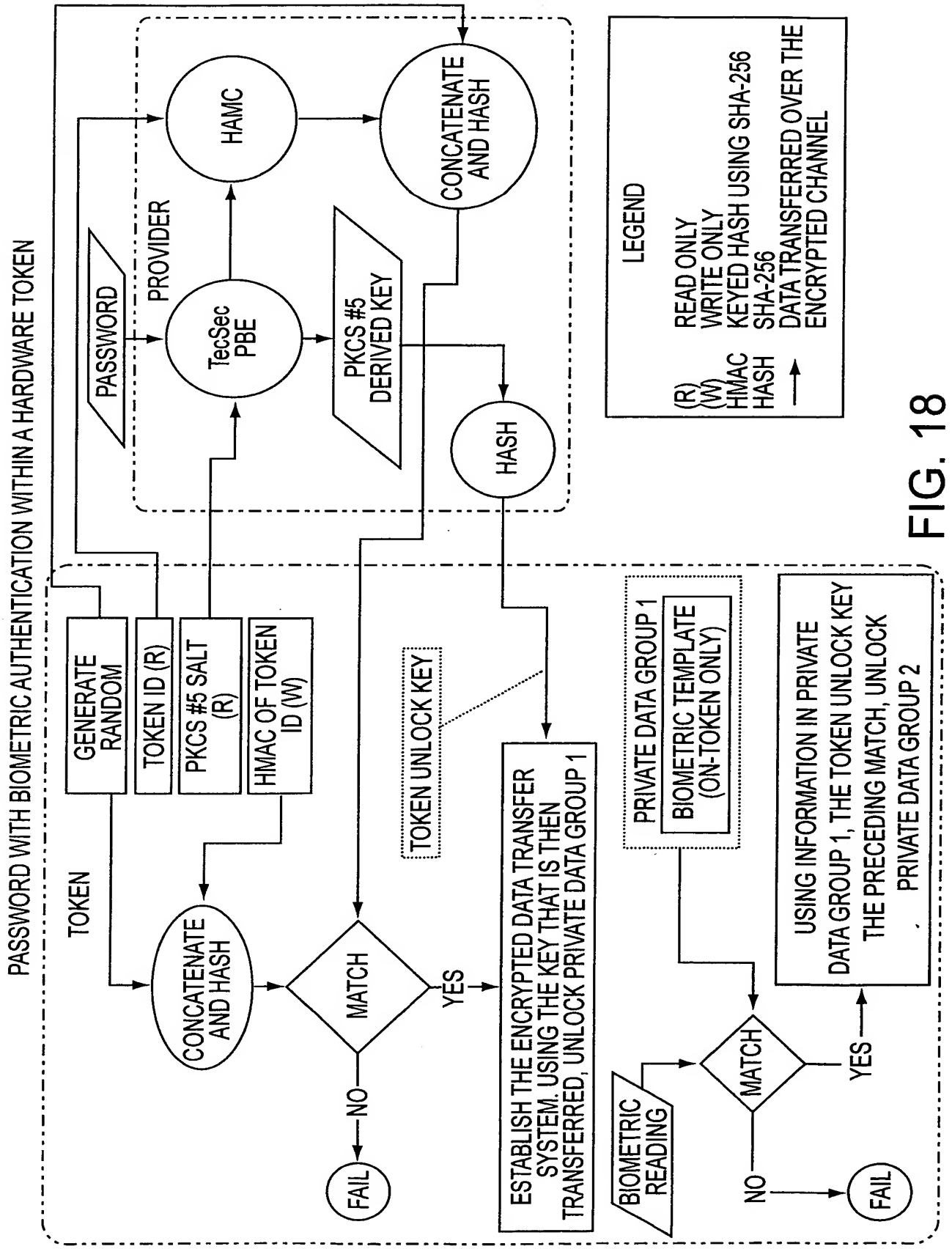

PASSWORD WITH BIOMETRIC AUTHENTICATION WITHIN A HARDWARE TOKEN
PROVIDER
PASSWORD
TecSec PBE
HAMC
CONCATENATE AND HASH
PKCS #5 DERIVED KEY
HASH
LEGEND
(R) READ ONLY
(W) WRITE ONLY
HMAC KEYED HASH USING SHA-256
HASH SHA-256
DATA TRANSFERRED OVER THE ENCRYPTED CHANNEL
TOKEN
GENERATE RANDOM
TOKEN ID (R)
PKCS #5 SALT (R)
HMAC OF TOKEN ID (W)
CONCATENATE AND HASH
MATCH
YES
NO
FAIL
TOKEN UNLOCK KEY
ESTABLISH THE ENCRYPTED DATA TRANSFER SYSTEM. USING THE KEY THAT IS THEN TRANSFERRED, UNLOCK PRIVATE DATA GROUP 1
PRIVATE DATA GROUP 1
BIOMETRIC TEMPLATE (ON-TOKEN ONLY)
BIOMETRIC READING
MATCH
NO
FAIL
YES
USING INFORMATION IN PRIVATE DATA GROUP 1, THE TOKEN UNLOCK KEY THE PRECEDING MATCH, UNLOCK PRIVATE DATA GROUP 2

FIG. 18

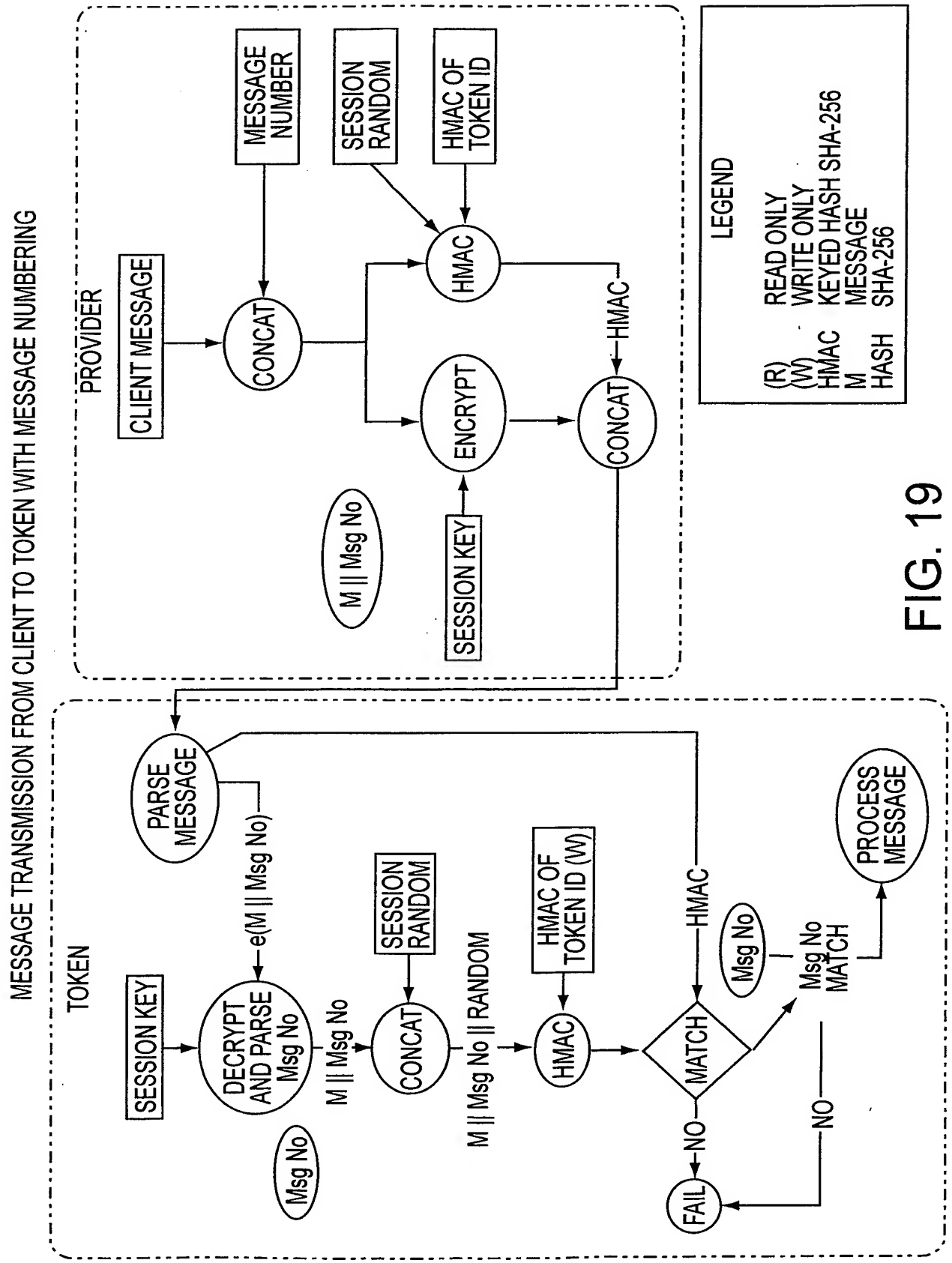

MESSAGE TRANSMISSION FROM CLIENT TO TOKEN WITH MESSAGE NUMBERING
PROVIDER
CLIENT MESSAGE
CONCAT
MESSAGE NUMBER
SESSION RANDOM
HMAC OF TOKEN ID
HMAC
ENCRYPT
CONCAT
HMAC
M || Msg No
SESSION KEY
LEGEND
(R) READ ONLY
(W) WRITE ONLY
HMAC KEYED HASH SHA-256
M MESSAGE
HASH SHA-256
TOKEN
PARSE MESSAGE
e(M || Msg No)
SESSION KEY
DECRYPT AND PARSE Msg No
Msg No
M || Msg No
SESSION RANDOM
CONCAT
M || Msg No || RANDOM
HMAC OF TOKEN ID (W)
HMAC
HMAC
MATCH
Msg No
Msg No MATCH
PROCESS MESSAGE
NO
FAIL
NO

FIG. 19

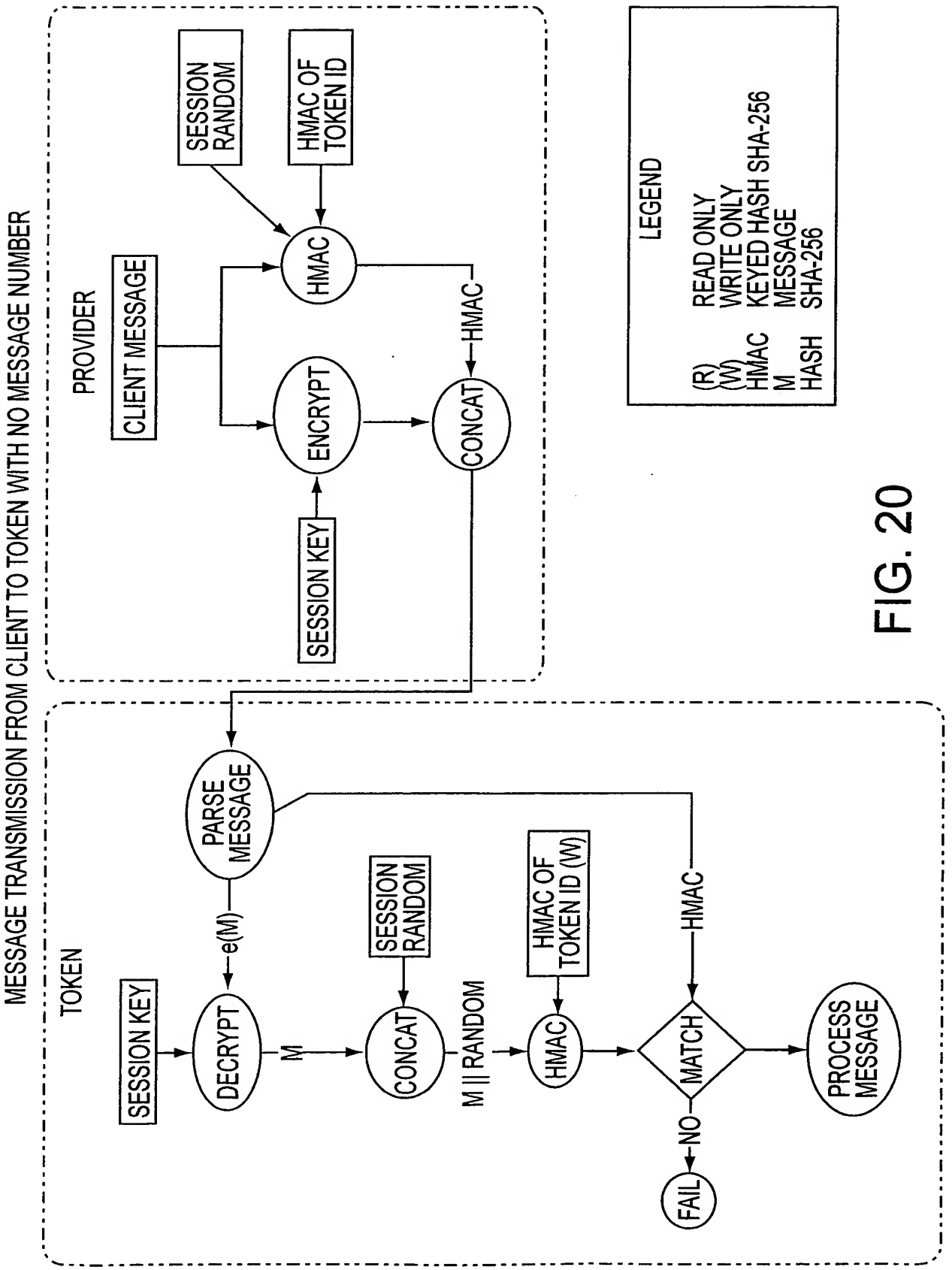

MESSAGE TRANSMISSION FROM CLIENT TO TOKEN WITH NO MESSAGE NUMBER
PROVIDER
CLIENT MESSAGE
SESSION RANDOM
HMAC OF TOKEN ID
HMAC
ENCRYPT
CONCAT
HMAC
SESSION KEY
LEGEND
(R) READ ONLY
(W) WRITE ONLY
HMAC KEYED HASH SHA-256
M MESSAGE
HASH SHA-256
TOKEN
SESSION KEY
DECRYPT
e(M)
M
PARSE MESSAGE
SESSION RANDOM
CONCAT
M || RANDOM
HMAC OF TOKEN ID (W)
HMAC
HMAC
MATCH
NO
FAIL
PROCESS MESSAGE

FIG. 20

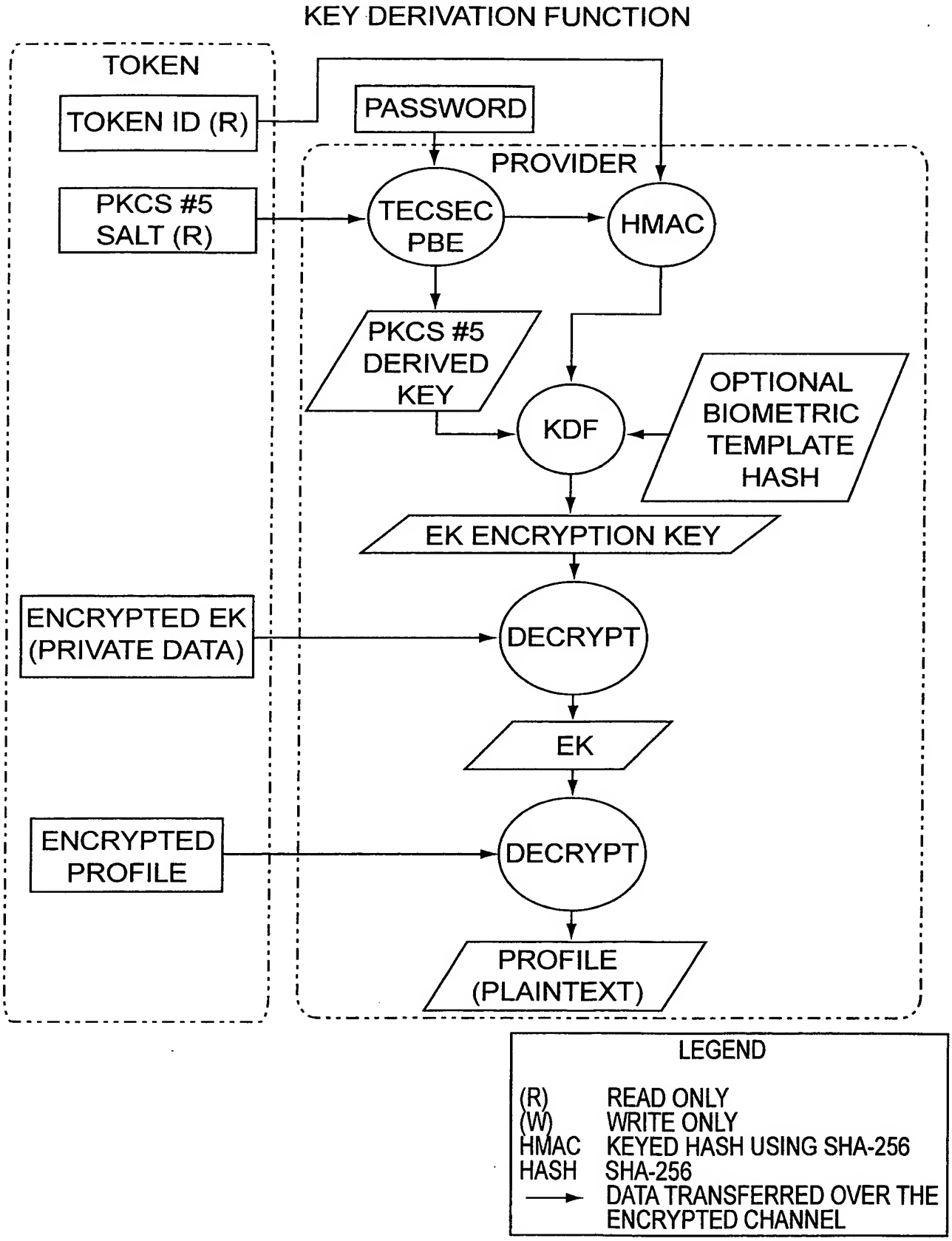

KEY DERIVATION FUNCTION
TOKEN
TOKEN ID (R)
PASSWORD
PROVIDER
PKCS #5 SALT (R)
TECSEC PBE
HMAC
PKCS #5 DERIVED KEY
OPTIONAL BIOMETRIC TEMPLATE HASH
KDF
EK ENCRYPTION KEY
ENCRYPTED EK (PRIVATE DATA)
DECRYPT
EK
ENCRYPTED PROFILE
DECRYPT
PROFILE (PLAINTEXT)
LEGEND
(R) READ ONLY
(W) WRITE ONLY
HMAC KEYED HASH USING SHA-256
HASH SHA-256
DATA TRANSFERRED OVER THE ENCRYPTED CHANNEL

FIG. 21

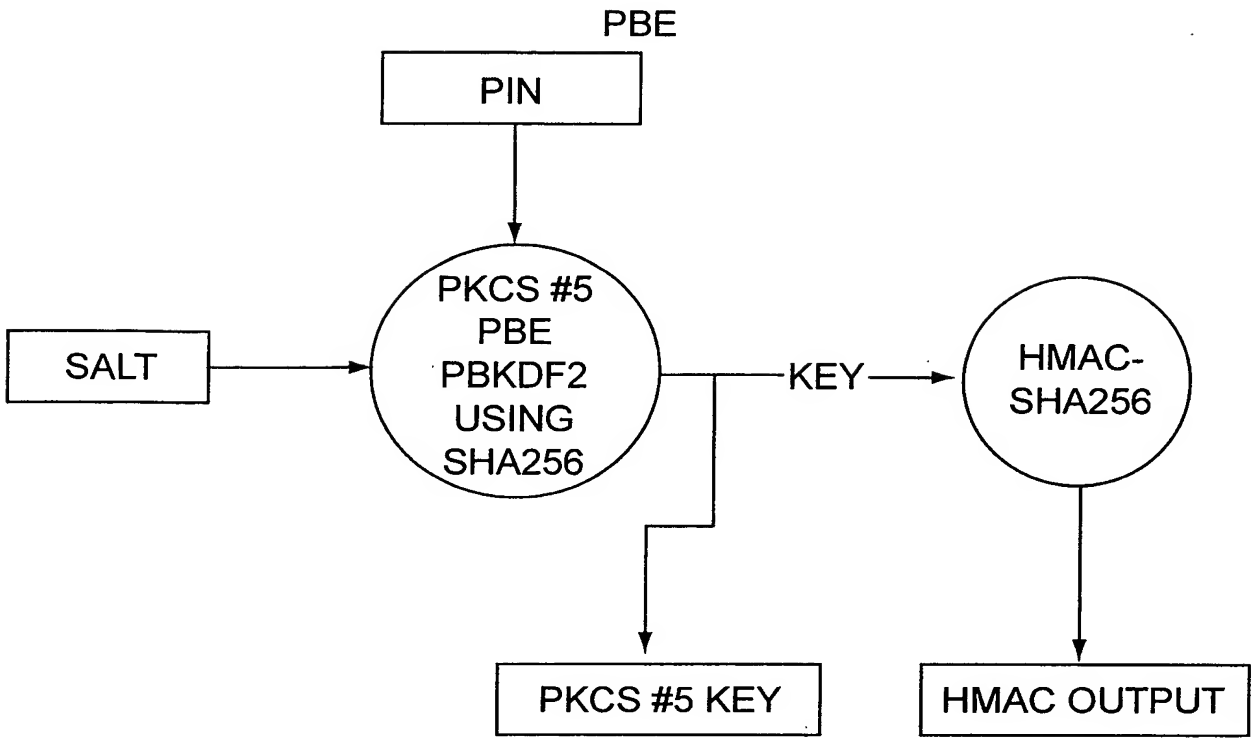

PBE
PIN
SALT
PKCS #5
PBE
PBKDF2
USING
SHA256
KEY
HMAC-
SHA256
PKCS #5 KEY
HMAC OUTPUT

FIG. 22